METHOD AND SYSTEM FOR DISTINGUISHING RELEVANT NETWORK SECURITY THREATS USING COMPARISON OF REFINED INTRUSION DETECTION AUDITS AND INTELLIGENT SECURITY ANALYSIS

ABSTRACT

An apparatus, a method, and a computer program are provided for distinguishing relevant security threats. With conventional computer systems, distinguishing security threats from actual security threats is a complex and difficult task because of the general inability to quantify a "threat." By the use of an intelligent conceptual clustering technique, threats can be accurately distinguished from benign behaviors. Thus, electronic commerce, and Information Technology systems generally, can be made safer without sacrificing efficiency.